

authority and control to ensure compliance with the regulations when acting as the Responsible Official.

(c) The Responsible Official must report the identification and final disposition of any select agent or toxin contained in a specimen presented for diagnosis or verification.

(1) The identification of any of the following select agents or toxins must be immediately reported by telephone, facsimile, or e-mail: *Bacillus anthracis*, Botulinum neurotoxins, Botulinum neurotoxin producing species of *Clostridium*, *Burkholderia mallei*, *Burkholderia pseudomallei*, *Francisella tularensis*, Ebola viruses, Marburg virus, Variola major virus (Smallpox virus), Variola minor (Alastrim), or *Yersinia pestis*. The final disposition of the agent or toxin must be reported by submission of APHIS/CDC Form 4 within seven calendar days after identification. A copy of the completed form must be maintained for three years.

(2) To report the identification and final disposition of any other select agent or toxin, APHIS/CDC Form 4 must be submitted within seven calendar days after identification. A copy of the completed form must be maintained for three years.

(3) Less stringent reporting may be required based on extraordinary circumstances, such as a widespread outbreak.

(d) The Responsible Official must report the identification and final disposition of any select agent or toxin contained in a specimen presented for proficiency testing. To report the identification and final disposition of a select agent or toxin, APHIS/CDC Form 4 must be submitted within 90 calendar days of receipt of the agent or toxin. A copy of the completed form must be maintained for three years.

[70 FR 13316, Mar. 18, 2005, as amended at 77 FR 61112, Oct. 5, 2012]

§ 73.10 Restricting access to select agents and toxins; security risk assessments.

(a) An individual or entity required to register under this part may not provide an individual access to a select agent or toxin, and an individual may not access a select agent or toxin, unless the individual is approved by the

HHS Secretary or Administrator, following a security risk assessment by the Attorney General.

(b) An individual will be deemed to have access at any point in time if the individual has possession of a select agent or toxin (e.g., ability to carry, use, or manipulate) or the ability to gain possession of a select agent or toxin.

(c) Each individual with access to select agents or toxins must have the appropriate education, training, and/or experience to handle or use such agents or toxins.

(d) To apply for access approval, each individual must submit the information necessary to conduct a security risk assessment to the Attorney General.

(e) A person with a valid approval from the HHS Secretary or Administrator to have access to select agents and toxins may request, through his or her Responsible Official, that the HHS Secretary or Administrator provide their approved access status to another registered individual or entity for a specified period of time.

(f) An individual's security risk assessment may be expedited upon written request by the Responsible Official and a showing of good cause (e.g., public health or agricultural emergencies, national security, or a short term visit by a prominent researcher). A written decision granting or denying the request will be issued.

(g) An individual's access approval will be denied or revoked if the individual is within any of the categories described in 18 U.S.C. 175b,

(h) An individual's access approval may be denied, limited, or revoked if:

(1) The individual is reasonably suspected by any Federal law enforcement or intelligence agency of committing a crime specified in 18 U.S.C. 2332b(g)(5), knowing involvement with an organization that engages in domestic or international terrorism (as defined in 18 U.S.C. 2331) or with any other organization that engages in intentional crimes of violence, or being an agent of a foreign power (as defined in 50 U.S.C. 1801), or

(2) It is determined such action is necessary to protect public health and safety.

§ 73.11

42 CFR Ch. I (10–1–13 Edition)

(i) An individual may appeal the HHS Secretary's decision to deny, limit, or revoke access approval under § 73.20.

(j) Access approval is valid for a maximum of three years.

(k) The Responsible Official must immediately notify CDC or APHIS when an individual's access to select agents or toxins is terminated by the entity and the reasons therefore.

[70 FR 13316, Mar. 18, 2005, as amended at 77 FR 61112, Oct. 5, 2012]

§ 73.11 Security.

(a) An individual or entity required to register under this part must develop and implement a written security plan. The security plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.

(b) The security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use. A current security plan must be submitted for initial registration, renewal of registration, or when requested.

(c) The security plan must:

(1) Describe procedures for physical security, inventory control, and information systems control,

(2) Contain provisions for the control of access to select agents and toxins, including the safeguarding of animals, including arthropods, or plants intentionally or accidentally exposed to or infected with a select agent, against unauthorized access, theft, loss or release.

(3) Contain provisions for routine cleaning, maintenance, and repairs,

(4) Establish procedures for removing unauthorized or suspicious persons,

(5) Describe procedures for addressing loss or compromise of keys, passwords, combinations, etc. and protocols for changing access numbers or locks following staff changes,

(6) Contain procedures for reporting unauthorized or suspicious persons or activities, loss or theft of select agents or toxins, release of select agents or toxins, or alteration of inventory records, and

(7) Contain provisions for ensuring that all individuals with access ap-

proval from the HHS Secretary or Administrator understand and comply with the security procedures.

(8) Describe procedures for how the Responsible Official will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins; and describe procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of such activity.

(9) Contain provisions for information security that:

(i) Ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit only authorized and authenticated users;

(ii) Ensure that authorized and authenticated users are only granted access to select agent and toxin related information, files, equipment (*e.g.*, servers or mass storage devices) and applications as necessary to fulfill their roles and responsibilities, and that access is modified when the user's roles and responsibilities change or when their access to select agents and toxins is suspended or revoked;

(iii) Ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to registered spaces in § 73.11 or records in § 73.17;

(iv) Establish a robust configuration management practice for information systems to include regular patching and updates made to operating systems and individual applications; and

(v) Establish procedures that provide backup security measures in the event that access control systems, surveillance devices, and/or systems that manage the requirements of section 17 of this part are rendered inoperable.

(10) Contain provisions and policies for shipping, receiving, and storage of select agents and toxins, including documented procedures for receiving, monitoring, and shipping of all select agents and toxins. These provisions must provide that an entity will properly secure containers on site and have